

Behind the Numbers: Privacy Practices on the Web

The state of privacy on the Internet is the topic of much discussion. Much of the focus to date has been on the numbers -- how many Web sites mention privacy? How many are allowing consumers the ability to opt-out? We believe it is time to focus on whether the policies in the marketplace reflect Fair Information Practices -- the corner stone of information privacy -- and perhaps more importantly, to decide whether they respond to consumers' privacy concerns.

In considering the state of privacy protection at commercial Web sites, this report takes a three-part approach.

- First, the report reviews survey data about individuals' expectations of privacy on the Internet and in commercial interactions. The survey data suggests that adherence to the Code of Fair Information Practices on the Internet would substantially address individuals' privacy concerns.
- Second, based upon the Georgetown Internet Privacy Policy Survey data, the report further analyzes the quality of privacy policies posted by some of the most frequently trafficked Web sites. The report finds that very few Web sites are abiding by the sub-set of Fair Information Practices called for by the Federal Trade Commission.
- Third, the report examines the private sector mechanisms for overseeing and enforcing privacy policies. The report finds that the seal programs -- BBBOnline, TRUSTe and WebTrust -- do not require companies to comply with the full set of Fair Information Practices and, because some programs have multiple versions, individuals must read the fine print if they want to know what protections and rights the programs afford them.

The report concludes that Fair Information Practices continue to be the exception rather than the rule on the World Wide Web; private sector enforcement programs cover a very small segment of commercial Web sites; and individuals' concerns with their privacy online remain only partially addressed.

I. What do we know about individuals' expectations of privacy?

Over the past four years we've witnessed an increase in surveys seeking to identify and document the public's attitudes toward privacy. Recent surveys document a growing concern with individual privacy on the Internet. Surveys have documented that the privacy of personal information is of critical concern to those on the Internet and those who have chosen not to come online. Surveys have also found a connection between individuals' willingness to engage in online commerce and their concerns with privacy. Privacy concerns continue to escalate with a recent report finding that nearly 90% of respondents were concerned about threats to their personal privacy online.

Privacy is becoming an increasingly important issue to Internet users.

- 87% of Net users are concerned about threats to their personal privacy while online. (*AT&T survey Beyond Concern: Understanding Net Users' Attitudes About Online Privacy, 1999*)
- Privacy now overshadows censorship as the number one most important issue facing the Internet. (*The 8th semi-annual poll of the Graphics, Visualization, and Usability Center at the Georgia Institute of Technology, 1997*)

- Tracking people's use of the Web (32%), and the sale of personal information (42%), were cited as the most pressing privacy issues on the Internet. (*Center for Democracy and Technology Privacy Survey, 1998*)
- A survey of parents found that their biggest concern overall, about their children's use of the Internet, was the abuse of personal information - an issue more troubling to them than credit card fraud, unsolicited email, and exposure to pornography and/or strangers. Sixty-five percent said that their children had been solicited to buy goods or services on the Web while more than half said their children have been asked to provide personal information at a site in order to access content.¹ (*FamilyPC Special Report: Annual FamilyPC Internet Survey Results, 1998*)

Privacy concerns hinder ecommerce.

- The majority of online users are not comfortable providing credit card (73%), financial (73%) or personal information (70%) to businesses online. (*National Consumers League, Consumers and the 21st Century, 1999*)
- Forty-two percent (42%) of those who access the Internet or the World Wide Web are using the Net only to gather information about products and services while a much smaller 24% are going online to purchase goods or services. (*National Consumers League, Consumers and the 21st Century, 1999*)
- Fifty-eight percent (58%) of consumers do not consider any financial transaction online to be safe, 67% are not confident conducting business with a company that can only be reached online, and 77% think it is unsafe to provide a credit card number over the computer. (*National Technology Readiness Survey, conducted by Rockridge Associates, 1999*)

- Many individuals have reported providing false information when registration is required. (*The 9th semi-annual poll of the Graphics, Visualization, and Usability Center at the Georgia Institute of Technology, 1998*)

Individuals want to know how their personal information is being used.

- Very strong majorities (91%) of Net users, and (96%) of those who buy products and services online, say that it is important for business Web sites to post notices explaining how they will use the personal information customers provide when buying products or services on the Web. (*AT&T survey, Beyond Concern: Understanding Net Users' Attitudes About Online Privacy, 1999*)
- 66.7% of respondents cite the lack of information about how their personal data will be used as the reason for not filling out registration forms online. (*The 10th semi-annual poll of the Graphics, Visualization, and Usability Center at the Georgia Institute of Technology, 1998*)
- 41.7% of Internet users want to know what information is being collected and 45.8% want to know how it will be used before they decide to withhold or supply demographic information. (*The 10th semi-annual poll of the Graphics, Visualization, and Usability Center at the Georgia Institute of Technology, 1998*)
- According to another survey, the most important factor to respondents in deciding whether to provide information is whether or not information will be shared with other companies and organizations. Other highly important factors in providing information on a Web site include whether information is used in an identifiable way, the kind of information collected, and the purpose

¹ The enactment, last October, of the Children's Online Privacy Protection Act addresses many of the privacy concerns raised by parents.

for which the information is collected. (*AT&T survey Beyond Concern: Understanding Net Users' Attitudes About Online Privacy, 1999*)

Individuals want control over how their personal information is used.

- 87% of respondents objected to a Web site selling information about them to other businesses. (AARP survey "AARP Members' Concerns About Information Privacy.)
- Similar concern was registered in the context of mergers, where 71% of respondents believed that merging companies should obtain written permission prior to sharing information. (AARP survey "AARP Members' Concerns About Information Privacy.)
- 74.3% of Internet users believe that content providers (Web sites) do not have the right to resell their personal information. (*The 10th semi-annual poll of the Graphics, Visualization, and Usability Center at the Georgia Institute of Technology, 1998*)
- 90.5% of Internet users believe that individuals should have complete control over which Web sites have access to demographic information. (The survey found individuals want control over the sale of their names and addresses by magazines to which they've subscribed.) (*The 10th semi-annual poll of the Graphics, Visualization, and Usability Center at the Georgia Institute of Technology, 1998*)

Internet users value their anonymity and are concerned about being tracked online.

- Individuals are often very uncomfortable providing identifiable information such as credit card numbers and social security numbers. (AT&T survey

Beyond Concern: Understanding Net Users' Attitudes About Online Privacy, 1999)

- 88% of Internet users say they value the ability to visit Web sites anonymously. (*The 10th semi-annual poll of the Graphics, Visualization, and Usability Center at the Georgia Institute of Technology, 1998*)
- 82.4% of Internet users disagree with the advertising agency practice of compiling usage behavior across Web sites for direct marketing purposes.
- Tracking people's use of the Web (32%) was cited as a pressing privacy concern on the Internet. (*Center for Democracy and Technology Privacy Survey, 1998*)

II. Privacy Expectations and Fair Information Practices

Individuals' privacy expectations, identified by the survey data above, are reflected in the Code of Fair Information Practices -- broadly recognized principles designed to ensure that individuals are able to "determine for themselves when, how, and to what extent information about them is shared."² Proposed in 1973 by a United States government advisory committee set up to examine the impact of computerized records on individual privacy,³ the Code has never been enacted as such, but remains a sound and enduring baseline for

² Alan Westin. *Privacy and Freedom* (New York: Atheneum, 1967), 7.

³ Report of the Secretary's Advisory Committee on Automated Personal Data Systems, Records, Computers and the Rights of Citizens, U.S. Dept. of Health, Education & Welfare, July 1973.

evaluating the information handling practices of businesses and the government.⁴

The Code of Fair Information Practices⁵ can be summarized as follows:

INDIVIDUAL RIGHTS

Access and Correction -- The individual has the right to see personal information about herself and to correct or remove data that is not timely, accurate, relevant, or complete.

Control -- The individual has the right to control the use of personal information. Personal information provided to a record keeper may not be used or disclosed for other purposes without the consent of the individual or other legal authority.

RECORD KEEPER RESPONSIBILITIES

Openness -- Record keepers who collect or maintain information about individuals must be publicly known, along with a description of the purpose and uses they make of personal information.

Limited Collection -- Record keepers who collect or maintain personal information must collect only what is necessary to support the purpose of collection. Personal information must be collected by lawful and fair means and, where appropriate, with the knowledge and consent of the individual.

Limited Use -- The use and disclosure of personal information must be limited to the purpose for which it was collected, unless the individual has granted consent.

⁴ Recent statements on protecting privacy from various branches of the United States government, such as the Department of Commerce's Guidelines for Effective Self-regulation, the Federal Trade Commission's 1998 Report to Congress, and the Children's Online Privacy Protection Act all center on elements of the Code.

⁵ Having discussed the Code of Fair Information Practices with many non-experts, we drafted this version in an effort to make it more accessible and self-explanatory. Comments and criticisms are welcome.

Data Quality -- Record keepers must ensure that personal information collected is relevant to the purpose of collection, accurate, timely, and complete.

Security -- Record keepers must institute reasonable security safeguards against such risks as loss, unauthorized access, destruction, use, modification and disclosure.

Accountability -- Record keepers must be accountable for complying with fair information practices.

Adherence to Fair Information Practices in the marketplace would address many of the documented privacy concerns of individuals in the online environment. The following section of the report examines the state of Fair Information Practices at commercial sites on the World Wide Web.

III. The Quality of Web Sites' Privacy Policies

What do we know about the quality of commercial Web sites privacy policies? Do they conform to Fair Information Practices? Two surveys conducted approximately a year apart give us some information about whether Web sites are posting privacy policies and, if they are, what these policies say.⁶ Using the data from the most recent survey conducted by Mary Culnan -- the Georgetown Internet Privacy Policy Study -- we can produce some useful information about the extent to which privacy policies are being posted and how closely they align with Fair Information Practices and the sub-set of Fair Information Practices that have been called for by the Federal Trade Commission -- Notice (openness); Choice (use and disclosure limitation); Access (access and correction); Security; and Enforcement (accountability).

⁶ Very little data is available about whether companies are adhering to the privacy policies they post.

A. Overview of the Reports

In June 1998, the Federal Trade Commission's "Privacy Online: A Report to Congress" found that despite increased pressure, businesses operating online continued to collect personal information without providing even a minimum of consumer protection. The report looked only at whether Web sites provided users with notice about how their data was to be used; there was no discussion of whether the stated privacy policies provided adequate protection. The survey found that, while 92% of the sites surveyed were collecting personally identifiable information, only 14% had some kind of disclosure of what they were doing. Approximately 1.9% of Web sites provided the type of notice that the FTC considered appropriate.

The newly released Georgetown Internet Privacy Policy Survey (GIPPS) provides new data. It finds that 92.8% of Web sites are collecting personally identifiable information and approximately 9.5 % of Web sites that collect personally identifiable information provide the type of notices called for by the FTC and required by the guidelines of the Online Privacy Alliance, the Better Business Bureau and TRUSTe. Approximately two-thirds of the sites made some statement about their collection or use of information -- for example "your order will be processed on our secure server" or "click here if you do not want to receive email from us" -- while one-third made no statements about privacy at all. The survey documented an increase in the number of Web sites collecting sensitive information such as credit card numbers (up 20%), names (up 13.3%), and even Social Security Numbers (up 1.7%).

B. A Closer Look at the Findings

The questions in the Georgetown Internet Privacy Policy Survey reflect a subset of Fair Information Practices. Regardless, the data provides some useful

information about the state of privacy practices on the Web. The survey data suggests that 1/3 of Web sites are silent on their use of personal information while 2/3's are taking some steps toward addressing users' privacy concerns, however, the policies being posted on the Web are far from complete.

- **Privacy policies are the exception not the rule on the Internet. Less than 10 % of Web sites are meeting the standards called for by the FTC and required by seal programs.**
- **While data is not available, based on the GIPPS survey we believe that few Web sites are adhering to the full set of Fair Information Practices.**
- **A small portion of Web sites participate in self-regulatory enforcement programs. According to CDT's analysis, only 8.5% of the sites surveyed (and a much smaller percentage of all sites on the World Wide Web) participate in one of the independent assessment programs discussed below.**
- **Roughly half of Web sites surveyed are providing visitors with *some* information about how personal information is collected, used, or disclosed.**
- **A third of Web sites are not providing individuals with any information about how personal data is handled.**
- **Approximately a third of Web sites surveyed are telling visitors about their use (or not) of cookies.**

- **Nearly 60 % of Web sites that collect information are providing individuals the *limited* ability to object to its use for re-contacting.**
- ***However*, no data is available about the number of Web sites that allow individuals to limit other uses of their personal information.**
- **Approximately 50 % of Web sites that collect information allow individuals to limit its disclosure to *third parties*.**
- ***However*, no survey data is available on whether Web sites allow individuals to limit disclosure to *affiliates* -- a growing concern in the privacy arena.**
- **45 % of Web sites inform consumers that their information is secure during transmission. But a smaller 18 % provide security assurances for information once it is collected.**

IV. Privacy Seal Programs -- oversight and enforcement

One proposal for overseeing and enforcing privacy practices in the private sector is the use of Seal programs. Generally, the programs emphasize providing consumers with: 1) notice of a companies practices; 2) the ability to opt-out of information sharing; and 3) assurance that appropriate security is used to protect their personal information. The programs center on a contract between the seal program and the licensed seal holder. The seal is issued in exchange for the company's agreement to abide by a specific set of standards for handling personal information and to permit some form of oversight of the agreement. All use the threat of seal revocation and, in certain cases, referral to appropriate legal authorities to assure compliance.

A. Overview

CDT examined three seal programs: BBBOnline; TRUSTe; and, WebTrust. As of January 1, 2000, the three seal programs will require licensees to comply with a similar subset of fair information principles. However, at the current time, the quality of privacy practices required of seal holders by the three programs varies substantially. Because two of the seal programs (TRUSTe and WebTrust) are in the process of raising their standards, a consumer cannot tell by the seal exactly what protections are offered. This undermines the simplicity the seals were intended to provide.

The BBBOnline seal relies on its well-recognized name and in-house dispute processes. The core of the BBBOnline program is a statement of compliance completed by companies and then reviewed by BBBOnline staff. BBBOnline staff initially handles disputes. If unsuccessful, the staff convenes a quasi-independent panel to hear the complaint, the findings of which are made public. Remedies for harmed consumers are decided on a case-by-case basis, but consumers cannot receive monetary damages. BBBOnline currently has 48 licensees and more than 400 applications are in process.

TRUSTe has recently revised its license agreement. Currently, consumers cannot tell by looking at the posted seal which standard a company is abiding by, creating the potential for consumer confusion. Licenses run a range between what is called the TRUSTe 3.0 agreement, through a set of 4.0 agreements to TRUSTe 5.0. The TRUSTe 3.0 agreement assures users of little more than the fact that companies are notifying consumers of their practices. By October 1999, all of the 3.0 agreements will expire, but until January 1, 2000, when all TRUSTe licensees will be adhering to the higher

(5.0) set of information practices, a TRUSTe seal could mean anything in between the 3.0 and 5.0 agreement. TRUSTe requires licensees to complete a self-certification statement that is reviewed by TRUSTe staff. To check compliance, TRUSTe seeds Web sites with personal information, conducts random spot checks of its licensees, and conducts independent audits in some instances. TRUSTe staff generally handles consumer complaints. There is no program for directly addressing the interests of aggrieved consumers. TRUSTe currently has 830 licensees and is receiving more than 100 applications a month.

WebTrust is in the process of revising its license agreement. Currently, the license emphasizes the security of the information practices and not privacy. By December 15, 1999, all licensees will be adhering to a higher set of fair information practice. In the meantime consumers must read the fine print. In addition to requiring a self-assessment by companies, WebTrust requires companies' policies and practices to be continually verified through on site audits by CPAs. An independent arbitration board handles disputes. The arbiter is free to award consumers whatever remedies are considered appropriate, including money. WebTrust has awarded 22 seals and at least 40 more are in process. 150 CPA firms worldwide are able to award seals.

Do the Seal programs require Web sites to adhere to Fair Information Practice Principles?

On A Five Star Scale ☆☆☆☆☆	BBBOnLine	TRUSTe 3.0 (TRUSTe has policies that range from 3.0 to 5.0. All 3.0 seals all expire by 10/99.)	TRUSTe 5.0 (Some members must follow this now, all will by 1/1/2000)	WebTrust 1.1 (All members currently follow this, beginning 9/15/1999 all members will gradually move to 2.0)	WebTrust 2.0 (All members will need to follow this by 12/15/1999)
Openness	☆☆☆☆	☆☆☆	☆☆☆☆	☆	☆☆☆☆
Access and Correction	☆☆☆	☆	☆☆		☆☆☆
Collection Limitation	☆		☆		
Data Quality	☆☆☆☆		☆☆☆☆		☆☆☆☆
Use Limitation	☆☆		☆☆		☆☆
Disclosure Limitation	☆☆		☆☆		☆☆
Security	☆☆☆		☆☆☆	☆☆☆☆	☆☆☆☆
Accountability*	☆☆	☆☆	☆☆	☆☆☆	☆☆☆

* Due to the newness of these programs assessing this element is difficult.

	BBBOnLine	TRUSTe 3.0 (TRUSTe has policies that range from 3.0 to 5.0. All 3.0 seals all expire by 10/99.)	TRUSTe 5.0 (Some members must follow this now, all will by 1/1/2000)	WebTrust 1.1 (All members currently follow this, beginning 9/15/1999 all members will gradually move to 2.0)	WebTrust 2.0 (All members will need to follow this by 12/15/1999)
Scope:					
Members' Web site privacy practices	Yes	Yes	Yes	No	Yes
Accepts complaints on non- member's Web site privacy practices	Yes	No	No	No	No
Members' privacy practices in e-commerce (other than Web activities)	No	No	No (considering different program)	No	No
Openness					
The policy must tell consumers:					
Purpose of information collection/ How information is used	Yes	Yes	Yes	No	Yes
What information is collected	Yes	Yes	Yes	No	Yes
Ability of individual to permit or limit other uses of personal information (opt-out, opt-in, etc)	Yes	Yes	Yes	No	Yes
Who information is shared with	Yes	Yes	Yes	No	Yes
Ability and means of correction	Yes	Yes	Yes	No	Yes
Contact information for company	Yes	Yes	Yes (more detailed)	Yes	Yes
Consequences of limiting uses of personal	Yes	Yes	Yes	No	Yes

information					
Security measures	Yes	Yes	Yes	Yes	Yes
Company Complaint Process	Yes	No	No	Yes	Yes

Individual Rights The company must provide consumers the following rights:					
The right to view personal information collected during Web site interactions held by the company	Yes	No	Yes	No	Yes
The right to correct this information if inaccurate	Yes (must be provided online)	No	Yes	No	Yes
Access to all personal information	No	No	No	No	No
The right to opt-out of some secondary uses of information	Yes	No	Yes	No	Yes
The right to opt-out of all secondary uses of personal information	No	No	Yes	No	Yes
The company assumes the following obligations:					
The duty to ensure personal information is accurate, complete and timely	Yes	No	Yes	No	Yes
The duty to limit the collection of personal information to that which is necessary to complete the transaction	No (addressed in children's seal)	No (addressed in children's seal)	No (addressed in children's seal)	No	No
The duty to protect personal information against unintended consequences	Yes	No	Yes	Yes	Yes
The duty to encrypt sensitive information (e.g. medical and financial information)	Yes	No	Yes	Yes	Yes
The duty to encrypt all personal information	No	No	No	Yes	Yes
The duty to test for viruses	No	No	No	Yes	Yes
The duty to ensure that third parties with whom they share data have similar security policies	Yes	No	No	Yes	Yes

The obligation to not use personal information submitted about others (such as the recipient of a package or gift) for secondary purposes	Yes (can use internal secondary purposes but not marketing nor third party sharing)	No	Yes	No	No
---	---	----	-----	----	----

To Participate the Company must:					
Complete a Pre-Registration Assessment	Yes	No	Yes	Yes (On-Site Review)	Yes (On-Site Review)
Agree to random checks on compliance (seeding/ random reviews)	Yes	Yes	Yes	No	No
Agree to Quarterly Reviews of their registration	No	Yes	Yes	Yes	Yes
Agree to Quarterly Onsite Reviews of their policies and practices	No	No	No	Yes- Quarterly On-Site Reviews by licensed CPAs	Yes – Quarterly On-Site Reviews by licensed CPAs
If a breach of policy is identified or consumer complains:					
The company will undergo an independent audit	Yes - on a case by case basis	Yes - on a case by case basis	Yes - on a case by case basis	Yes	Yes
Harmed Consumers will be notified	Not generally. But may occur on a case-by-case basis.	Not generally. But may occur on a case-by-case basis.	Not generally. But may occur on a case-by-case basis.	Not generally. But may occur on a case-by-case basis.	Not generally. But may occur on a case-by-case basis.
Seal may be pulled if violation is not addressed or reoccurs	Yes	Yes	Yes	Yes	Yes
Proper Authorities may be notified	Yes	Yes	Yes	Yes	Yes
The company must participate in a Dispute Resolution	Yes (quasi-	No	No	Yes	Yes

program	independent)			(Independent)	(Independent)
Dispute Resolutions findings are public	Yes	Maybe (case by case)	Maybe (case by case)	No	No
If an individual is found to be harmed are they compensated?	Yes (no monetary damages are awarded)	No	No	Yes (damages, including monetary damages may be awarded)	Yes (damages, including monetary damages may be awarded)

B. Do the Seal programs ensure compliance with Fair Information Practices? Can individuals enforce their privacy rights?

While the Seal programs' standards are, according to the GIPPS, higher than the current practices at the vast majority of Web sites, they fall short of meeting the Fair Information Practice Principles. As stated above, enforcement program participants make up only a small portion of the Web sites online. And even if a site is a member of a seal program, consumers should be wary -- for today understanding what a seal means requires reading the fine print. Two sites with the same seal could have vastly different policies. While the seal programs will each have a single standard for companies to meet by January 2000, today it is clearly wise to be cautious. Even with standardized requirements consumers will have to read the small print to find out the practices of a specific site and exactly what rights they may or may not have.

In addition, as a recent complaint against Microsoft filed with TRUSTe illustrated the scope of the self-regulatory enforcement programs is narrow. They only have the ability to monitor and enforce privacy practices on the companies Web site. Where a consumer has an online, but not Web site based, privacy complaint or an offline privacy complaint, the seal programs are unable to address them.

The threat of seal revocation is likely to encourage participants to more actively monitor their own behavior to ensure compliance, however seal revocation does not provide the individual who is harmed with relief. At this time it is unclear whether the private sector mechanisms for addressing consumer complaints and handling disputes will provide individuals with an effective method of protecting their privacy.

Overall, the Seal programs have raised the bar in the private sector by establishing stronger -- but still short of complete -- practices for handling personal information. However, they fall short of meeting the Fair Information Practice Standards and responding to consumers' concerns. Today the three programs have enrolled a total of 900 Web sites -- a very small slice of the hundreds of thousand commercial sites on the World Wide Web.

V. Conclusions and Recommendations

Whether the measuring tool is the policies of the Online Privacy Alliance, the seal programs, the FTC's pared down version of the Code of Fair Information Practices, or the full Code of Fair Information Practices, -- privacy practices at the vast majority of commercial Web sites are not making the mark.

The survey data above documented specific concerns of individuals using the Internet. In analyzing the state of privacy practices on the Web, it appears that consumers concerns are receiving an incomplete response from Web sites. 87% of individuals stated a concern with their privacy online -- but a third of highly trafficked Web sites remain completely silent on how they handle personal information. 91% of Internet users, and (96%) of those engaged in ecommerce want to know what personal information is collected and used -- but less than 50% of frequently trafficked Web sites provide individuals with this information. An overwhelming majority of individuals want to decide how their information is used -- but 40% of business Web sites are not allowing individuals to exercise even a limited right to object to companies recontacting them. 74.3% of Internet users believe that content providers (Web sites) do not have the right to resell their personal information -- but of the 53% highly trafficked Web sites that say they share or sell personal information less than 50% allow consumers to opt-out of this practice. Individuals are concerned about their use of the World Wide Web being tracked and profiled -- but only 31% of these high traffic Web sites

informed individuals about their use (or non-use) of cookies. Consumers are not being provided with adequate information about the use of personal information and they are not being provided with the ability to determine for themselves how their personal information is used.

The seal programs have improved their requirements, however they too fall short of the Code of Fair Information Practices. And together their reach continues to be quite small -- covering approximately 900 Web sites. It remains unlikely that the "bad actors" will participate in self-regulatory programs. A ubiquitous oversight and enforcement program has not emerged.

In light of these statistics on the behavior of highly trafficked Web sites, consumers have good reason to be concerned for their privacy online. Thanks to the actions of leading companies, privacy and consumer advocates, and various parts of the government, *some* progress is evident on all fronts. However ubiquitous and enforceable privacy protections across the World Wide Web have not materialized. We continue to believe that legislation is both necessary and inevitable to make individual privacy on the Internet the rule rather than the exception. We believe that the GIPPS survey data indicates that many Web sites need some baseline policy guidance. The relatively low participation in self-enforcement programs indicates that, on their own, they will not be a viable option for the vast majority individuals with privacy complaints. If we fail to create a privacy framework that addresses individuals' privacy concerns we stand to undermine its enormous potential to support a vital online community and marketplace.